государственное бюджетное профессиональное образовательное учреждение
«Пермский химико-технологический техникум»

Одобрено на заседании ПЦК
Информационных технологий и
программирования
Протокол № 9 от 13.06.2018

УТВЕРЖДАЮ
Заместитель директора
_____ О.В.Князева

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Защита информации техническими средствами

для специальности

10.02.05 Обеспечение информационной безопасности
автоматизированных систем

2018

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее - СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем**,** утверждённым приказом Министерства образования и науки Российской Федерации 09 декабря 2016 № 1553, зарегистрированным в Министерстве юстиции Российской Федерации 26 декабря 2016 года, регистрационный № 44936, входящим в укрупнённую группу специальностей 10.00.00 Информационная безопасность

Составители: Юшкова Евгения Владимировна

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Защита информации техническими средствами

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля (далее – рабочая программа) – является частью основной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников в области информатики и вычислительной техники при наличии основного общего и среднего (полного) общего образования.

1.2. Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт в:

- выявлении технических каналов утечки информации;
- применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;
- проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
- проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

уметь:

- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
- применять технические средства для криптографической защиты информации конфиденциального характера;
- применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;
- применять инженерно-технические средства физической защиты объектов информатизации.

знать:

- физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;
- основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;
- основные способы физической защиты объектов информатизации;
- методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
- номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

1.3. Количество часов на освоение программы профессионального модуля

Вид учебной деятельности	**Объем часов**
Всего объем образовательной нагрузки	542
в том числе:	
Во взаимодействии с преподавателем	524
всего по дисциплинам и МДК	272
учебная практика	36
производственная практика	180
курсовое проектирование	--
консультации	14
промежуточная аттестация	22
Самостоятельная работа студента: 1. Подготовка докладов и сообщений 2. Подготовка к промежуточной аттестации	18
Промежуточная аттестация в форме	Экзамен квалификационный

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности *Защита информации техническими средствами*, в том числе профессиональными (ПК), указанными в ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Код	Наименование результата обучения
ВД 3	**Защита информации техническими средствами**
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

В процессе освоения ПМ студенты должны овладеть общими компетенциями (ОК):

ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

3.1. Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего объем образовательной нагрузки	Работа обучающихся во взаимодействии с преподавателем								Самостоятельная работа обучающегося	
			Объем времени, отведенный на освоение междисциплинарного курса (курсов)				Практика		Консультации, час	Промежуточная аттестация, час	Всего, часов	в т.ч., курсовая работа (проект), часов
			Всего, часов	*в т.ч. теоретическое обучение, часов*	в т.ч. лабораторные работы и практические занятия, часов	курсовая работа (проект), часов	Учебная, часов	Производственная (по профилю специальности)				
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
ПК 3.1-ПК 3.4, ОК 01-ОК 10	Раздел 1. Техническая защита информации	**158**	136	78	58				6	8	**8**	
ПК 3.5, ОК 01-ОК 10	Раздел 2. Инженерно-технические средства физической защиты объектов информации	**154**	136	72	64				4	4	**10**	
	Учебная практика	**38**					36			2		
ПК 3.1-3.5, ОК 01-ОК 10	Практика производственная	**186**						180	4	2		
	Экзамен квалификационный	**6**								6		
	Всего:	**542**	**272**	**150**	**122**	**0**	**36**	**180**	**14**	**22**	**18**	**0**

3.2. Содержание обучения по профессиональному модулю ПМ.03 Защита информации техническими средствами

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов			Уровень освоения
		лек	пр	сам	
1	2	3	4	5	6
Раздел 1 модуля. Применение технической защиты информации		**78**	**58**	**8**	
МДК.03.01 Техническая защита информации		**78**	**58**	**8**	
Подраздел 1.1. Концепция инженерно-технической защиты информации					
Тема 1.1.1. Предмет и задачи технической защиты информации	**Содержание**	4			1
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.				
Тема 1.1.2. Общие положения защиты информации техническими средствами	**Содержание**	4			
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.				
Подраздел 1.2. Теоретические основы инженерно-технической защиты информации					
Тема 1.2.1. Информация как предмет защиты	**Содержание**	4			
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.				
	Практические занятия		2		
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.				
Тема 1.2.2. Технические каналы утечки информации	**Содержание**	4			2
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических				

	каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.				
	Практические занятия		2		
	Классификация существующих физических полей и технических каналов утечки информации.				
Тема 1.2.3. Методы и средства технической разведки	**Содержание**	4			
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.				
	Практические занятия		2		
	Определении степени защищенности объекта информатизации путем моделирования возможных действий технических разведок. Определение потенциальных и реальных каналов утечки информации.				
Подраздел 1.3. Физические основы технической защиты информации					
Тема 1.3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	6			
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей				
	Практические занятия		4		
	Измерение параметров физических полей				
Тема 1.3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	4			
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.				
Подраздел 1.4. Системы защиты от утечки информации					
Тема 1.4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	4			
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому				2

	каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.				
	Практические занятия		2		
	Защита от утечки по акустическому каналу				
Тема 1.4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	4			
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.				
	Практические занятия		2		
	Работа остронаправленных микрофонов. Работа диктофонов со скрытой записью.				
Тема 1.4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	6			
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.				
	Практические занятия		4		
	Защита от утечки по виброакустическому каналу				
Тема 1.4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	4			
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.				
	Практические занятия		4		
	Определение каналов утечки ПЭМИН				
	Защита от утечки по цепям электропитания и заземления				
Тема 1.4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	4			
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств				2

	защиты информации от несанкционированной утечки по телефонному каналу.				
	Практические занятия		4		
	Работа скремблеров и вокодеров				
Тема 1.4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	6			
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.				
	Практические занятия		4		
	Активное подавление сигналов радиолокаторов. Защита от утечки информации по электросетевому каналу.				
Промежуточная аттестация по МДК.03.01 (экзамен)		**6**			
Тема 1.4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	2			
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.				
	Практические занятия		8		
	Маскировка в видимом и ИК диапазона света. Способы и средства видеоконтроля.				
Подраздел 1.5. Применение и эксплуатация технических средств защиты информации					
Тема 1.5.1. Применение технических средств защиты информации	**Содержание**	8			2
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.				
	Практические занятия		10		
	Представление моделей объектов информационной безопасности. Определение путей проникновения злоумышленника к источнику информации. Типовые индикаторы каналов утечки. Комплексная система защиты.				
Тема 1.5.2. Эксплуатация технических средств защиты информации	**Содержание**	10			
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации.				

	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.				
	Практические занятия		10		
	Комплексы обнаружения и пеленгации. Анализаторы телефонных линий. Гарантированное уничтожение информации на магнитных носителях.				
Тематика самостоятельной работы при изучении МДК.03.01 1. Направление комплексного проектирования системы защиты информации 2. Основные проблемы реализации системы защиты информации 3. Требования к КСЗИ 4. Задачи стратегии защиты информации 5. Верификация 6. Дискретный контроль доступа 7. Биометрическая идентификация 8. Биометрия по клавиатурному почерку 9. Классификация признаков голоса и речи 10. Средства высоконадежной биометрической аутентификации 11. Шпионаж, сбор служебной информации, сканирование эфира, обработка неуточненных источников 12. Меры по защите информации внутри зоны 13. Автоматическое обнаружение движущегося нарушителя 14. Контроль эффективности инженерно-технической защиты информации 15. Физические основы побочных излучений и наводок				8	
Промежуточная аттестация по МДК.03.01					2
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		**72**	**64**	**10**	
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**72**	**64**	**10**	
Подраздел 2.1. Построение и основные характеристики инженерно-технических средств физической защиты					
Тема 2.1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	8			
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.				

	Тематика практических занятий и лабораторных работ		8		
	Практическая работа №1. Характеристика объекта защиты Выбор объекта защиты Составление плана кабинета как объекта защиты Построение пространственной модели объекта защиты Определение категории защищаемого объекта				
Тема 2.1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	10			
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.				
	Практические занятия		4		
	Практическая работа №2. Формирование требований к физической защите объекта Анализ нормативно-правовых документов Формирование перечня требований к защите объекта Определение количества рубежей защиты				
Подраздел 2.2. Основные компоненты комплекса инженерно-технических средств физической защиты					
Тема 2.2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	8			
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.				
	Практические занятия		8		
	Практическая работа №3. Монтаж датчиков пожарной и охранной сигнализации				
Тема 2.2.2. Система контроля и управления доступом	**Содержание**	10			
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования				

	СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.				
	Практические занятия		8		
	Практическая работа №4. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя				
	Практическая работа №5. Рассмотрение принципов устройства, работы и применения средств контроля доступа				
Тема 2.2.3. Система телевизионного наблюдения	**Содержание**	12			
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.				
	Практические занятия		6		
	Практическая работа №6. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.				
Промежуточная аттестация по МДК.03.02 (дифференцированный зачет)		**2**			
Тема 2.2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	6			
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.				
	Практические занятия		6		
	Практическая работа №7. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.				
Тема 2.2.5 Система воздействия	**Содержание**	6			
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.				
	Практические занятия		8		
	Практическая работа №8. Выбор и обоснование средств подсистемы задержки Исследование технических средств взаимодействия				
Подраздел 2.3. Применение и эксплуатация инженерно-технических средств физической защиты					
Тема 2.3.1 Применение инженерно-	**Содержание**	6			
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления				

технических средств физической защиты	доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.				
	Практические занятия		8		
	Практическая работа №9. Разработка структурной схемы и спецификации оборудования Представление моделей объектов информационной безопасности. Разработка спецификации оборудования физической защиты объекта				
Тема 2.3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	6			
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.				
	Практические занятия		8		
	Практическая работа №10. Эксплуатация инженерно-технических средств физической защиты Изучение принципов диагностики. Устранение отказов и восстановление работоспособности технических средств физической защиты				
Тематика самостоятельной работы при изучении МДК.03.02 – Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. – Размещение периметровых средств обнаружения на местности. – Самостоятельнее изучения порядка допуска субъектов на охраняемые объекты.				10	
Промежуточная аттестация по МДК.03.02		**2**			
Учебная практика **Виды работ:** – Измерение параметров физических полей. – Определение каналов утечки ПЭМИН. – Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. – Установка и настройка технических средств защиты информации.			**36**		

– Проведение измерений параметров побочных электромагнитных излучений и наводок. – Проведение аттестации объектов информатизации. – Монтаж различных типов датчиков. – Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. – Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. – Рассмотрение системы контроля и управления доступом. – Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. – Рассмотрение датчиков периметра, их принципов работы. – Выполнение звукоизоляции помещений системы зашумления. – Реализация защиты от утечки по цепям электропитания и заземления. – Разработка организационных и технических мероприятий по заданию преподавателя; – Разработка основной документации по инженерно-технической защите информации.				
Промежуточная аттестация по учебной практике	**2**			
Производственная практика профессионального модуля **Виды работ** – Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; – Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; – Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; – Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.		**180**		
Промежуточная аттестация по производственной практике	**2**			
Экзамен по профессиональному модулю	**6**			
Консультирование	**14**			
Всего	**542**			

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Лекционные аудитории с мультимедийным оборудованием; лаборатории «Технических средств защиты информации», «Сетей и систем передачи информации».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест – не менее 30, рабочее место преподавателя, проектор, персональный компьютер, интерактивная доска, комплект презентаций.

Оборудование лаборатории «Технических средств защиты информации» и рабочих мест лаборатории:

1. Стол преподавателя – 1 шт.
2. Стул преподавателя – 1 шт.
3. Столы ученические – 3 шт.
4. Стулья – 15 шт.
5. Доска магнитная классная – 1 шт.
6. Персональный компьютер – 1 шт.
7. Виртуальный тренажёр "Аттестация объекта по требованиям защиты от утечек информации по техническим каналам" (лицензия на 1 рабочее место), ТЗИ-ВИРТ-СРТФ
8. Учебный стенд системы видеонаблюдения, в составе:
    a. Камера купольная внутренняя AHD
    b. Камера купольная поворотная AHD
    c. Камера купольная поворотная IP
    d. Гибридный видеорегистратор
    e. Маршрутизатор
    f. АКБ 12 а\ч
    g. Персональный компьютер
9. Учебный стенд СКУД, в составе:

a. Контроллер СКУД
b. Настольный считыватель 4 в 1
c. Терминал распознавания лиц
d. АКБ 12 а\ч
e. Неуправляемый коммутатор
f. Карточка Mifare АйТек ПРО
g. Карточка Proximity EM-Marine (тонкая)
h. Замок электромагнитный
i. Защелка электромеханическая
j. Имитатор привода ворот
k. Комплект для радиоуправления до 100м.
l. Имитатор турникета
m. ПО RusGuard Soft
n. Персональный компьютер

Программное обеспечение:

ОС Windows 10, Архиватор WinRAR, Приложения MS Office 2016, Adobe Reader X, Notepad++, Google Chrome, Консультант Плюс, Oracle VM Virtual Box, ItMan, ОС Linux: Lubuntu и Kali Linux

Оборудование лаборатории «Сетей и систем передачи информации» и рабочих мест лаборатории:

1. Стол преподавателя – 1 шт.
2. Стул преподавателя – 1 шт.
3. Столы ученические – 3 шт.
4. Стулья – 15 шт.
5. Доска магнитная классная – 1 шт.
6. Персональный компьютер – 1 шт.
7. Учебный стенд Сетевые технологии, в составе:
    a. Стойка 19"
    b. Аппаратный брандмауэр
    c. Управляемый коммутатор уровня 3

d. Управляемый коммутатор уровня 2
e. Неуправляемый коммутатор
f. Беспроводной маршрутизатор
g. Коммутационная панель SNR, 19"
h. Интегрированный вычислительный узел
i. Сервер

Программное обеспечение:

ОС Windows 10, Архиватор WinRAR, Приложения MS Office 2016, Adobe Reader X, Notepad++, Google Chrome, Консультант Плюс, Oracle VM Virtual Box, ItMan, ОС Linux: Lubuntu и Kali Linux, Комплексная система защиты корпоративной сети

Реализация рабочей программы ПМ предполагает учебную и производственную практику, которая может проводиться концентрировано или рассредоточено.

4.2. Информационное обеспечение обучения

Основные источники

1. Скрипник Д.А. Общие вопросы технической защиты информации: курс лекций / Скрипник Д.А. — Москва: Интуит НОУ, 2016. — 424 с. — URL: https://book.ru/book/917804. — Текст: электронный.
2. Сагдеев К.М. Физические основы защиты информации Бакалавриат: учебное пособие / Сагдеев К.М., Петренко В.И., Чипига А.Ф. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 394 с. — URL: https://book.ru/book/928736. — Текст: электронный.

Дополнительные источники:

1. Гребенюк Е.И. Технические средства информатизации: учебник для студентов СПО / Е.И. Гребенюк, Н.А. Гребенюк. - М.: Издательский центр "Академия", 2014г.

2. Лавровская О.Б. Технические средства информатизации. Практикум: учебное пособие для студентов СПО. - М.: Издательский центр "Академия", 2013г.
3. Руденков Н.А. Технологии защиты информации в компьютерных сетях: курс лекций / Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суровов А.М. — Москва : Интуит НОУ, 2016. — 368 с. — URL: https://book.ru/book/918258. — Текст: электронный
4. Тараскин М.М. Комплексная защита информации в организации: монография / Тараскин М.М., и др. — Москва: Русайнс, 2017. — 353 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/922538. — Текст: электронный
5. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
7. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
8. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
9. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
10. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
11. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
12. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

13. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
14. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
15. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
16. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
17. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
18. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
19. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
20. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

21. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
22. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
23. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
24. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
25. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
26. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
27. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
28. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
29. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

30. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
31. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
32. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
33. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
34. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
35. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
36. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
37. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
38. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
39. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
40. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

41. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
42. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
43. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
44. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
45. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
46. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
47. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
48. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
49. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

50. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
51. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
52. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
53. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
54. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Интернет - источники

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru

4.3. Общие требования к организации образовательного процесса

Освоение ПМ.03 Защита информации техническими средствами производится в соответствии с учебном планом по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и календарным графиком.

Образовательный процесс организуется строго по расписанию занятий, утвержденному заместителем директора. График освоения ПМ предполагает последовательное освоение МДК.03.01 Техническая защита информации, МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации, включающих в себя как теоретические, так и практические занятия.

Освоению ПМ предшествует обязательное изучение учебных дисциплин «Технические средства информатизации» и «Основы информационной безопасности».

Изучение теоретического материала может проводиться как в каждой группе, так и для нескольких групп (при наличии нескольких групп на специальности).

При проведении практических занятий проводится деление группы обучающихся на подгруппы, численностью не более 13 чел. Практические работы проводятся в специально оборудованной лаборатории технических средств защиты информации, сетей и систем передачи информации.

В процессе освоения ПМ предполагается проведение текущего и промежуточного контроля знаний, умений у студентов. Промежуточная аттестация по междисциплинарным курсам модуля является обязательной для всех обучающихся. Формой промежуточной аттестации по МДК.03.01 Техническая защита информации является экзамен в 6 семестре и дифференцированный зачёт в 7 семестре, по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации –

дифференцированный зачет в 6 и 7 семестрах. Результатом освоения ПМ выступают профессиональные компетенции, оценка которых представляет собой создание и сбор свидетельств деятельности на основе заранее определенных критериев.

С целью оказания помощи обучающимся при освоении теоретического и практического материала, выполнения самостоятельной работы разрабатываются учебно-методические комплексы.

С целью методического обеспечения прохождения учебной и производственной практики, разрабатываются методические рекомендации для обучающихся.

При освоении ПМ каждым преподавателем устанавливаются часы дополнительных занятий, в рамках которых для всех желающих проводятся консультации.

Текущий учет результатов освоения ПМ производится в журнале успеваемости.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по МДК:

наличие высшего профессионального образования, соответствующего профилю специальности, стажировка по профилю специальности не реже 1 раза в 3 года.

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих проведение практических работ:

наличие высшего профессионального образования, соответствующего профилю специальности, стажировка по профилю специальности не реже 1 раза в 3 года.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой:

наличие высшего профессионального образования, соответствующего профилю специальности, стажировка по профилю специальности не реже 1 раза в 3 года.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Коды проверяемых компетенций	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации –	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Коды проверяемых компетенций	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– распознает задачу и/или проблему в профессиональном контексте; – анализирует задачу и/или проблему и выделяет её составные части; – определяет этапы решения задачи; – выявляет и осуществляет поиск информации, необходимой для решения задачи и/или проблемы; – составляет план действия; определяет необходимые ресурсы; – владеет актуальными методами работы в профессиональной и смежных сферах; – реализует составленный план; – оценивает результат и последствия своих действий, выделяет в нём сильные и слабые стороны	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач Экспертная оценка документов по учебной и производственной практике

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	– определяет задачи поиска информации; – определяет необходимые источники информации; – планирует процесс поиска; – структурирует получаемую информацию в соответствии с параметрами поиска; – выделяет наиболее значимое в перечне информации; – оценивает практическую значимость результатов поиска; – интерпретирует полученную информацию в контексте профессиональной деятельности; – оформляет результаты поиска	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач Экспертная оценка документов по учебной и производственной практике
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	– использует актуальную нормативно-правовую документацию по специальности; – применяет современную научно профессиональную терминологию; – определяет актуальность нормативно-правовой документации в профессиональной деятельности; – выстраивает траектории профессионального и личностного развития; – участвует в конкурсах профессионального мастерства; – участвует в мероприятиях профессиональной направленности (вебинары, семинары, конференции, круглые столы, форумы и т.д.)	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Экспертная оценка портфолио. Экспертная оценка документов по учебной и производственной практике
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	– участвует в деловом общении для эффективного решения деловых задач; – планирует профессиональную деятельность; – организует работу коллектива и команды; – взаимодействует с коллегами, руководством, клиентами; – при групповом обсуждении задает вопросы для понимания идей других; – при групповом обсуждении: убеждается, что коллеги по группе поняли предложенную идею; – участвует в деятельности по выявлению ресурсов команды;	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Наблюдение за выполнением групповых проектных работ. Экспертная оценка документов по учебной и производственной практике

	– анализирует работу членов группы; – анализирует результаты выполненного задания; – презентует результаты работы группы; – защищает полученные командой результаты	
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	– грамотно (устно и письменно) излагает свои мысли по профессиональной тематике на государственном языке; – проявляет толерантность в рабочем коллективе; – извлекает из устной речи (монолог, диалог, дискуссия) нужную информацию и логические связи, организующие эту информацию; – грамотно оформляет документы на государственном языке; – корректно общается с преподавателями и одногруппниками; – соблюдает заданный жанр высказывания (служебный доклад, выступление на совещании / собрании, презентация товара / услуг); – корректно отвечает на вопросы, направленные на выяснение мнения (позиции); – задает четко сформулированные вопросы, направленные на получение необходимой информации.	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач. Экспертная оценка документов по учебной и производственной практике.
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.	– соблюдает нормы поведения во время учебных занятий и прохождения учебной и производственной практик; – понимать значимость своей специальности; – демонстрирует поведение на основе общечеловеческих ценностей	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Экспертная оценка документов по учебной и производственной практике
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных	– эффективность выполнения правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик; – использует ресурсосберегающие	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Экспертная оценка

ситуациях.	технологии в профессиональной деятельности, на рабочем месте.	документов по учебной и производственной практике
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	– эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик – участие в спортивных мероприятиях и/или мероприятиях направленных на формирование здорового образа жизни	Наблюдение за обучающимся во время прохождения учебной и производственной практики. Экспертная оценка портфолио
ОК 9. Использовать информационные технологии в профессиональной деятельности.	– ориентируется в информационно-коммуникационных технологиях, применяемых в профессиональной деятельности; – применяет средства информатизации и информационных технологий для реализации профессиональной деятельности; – в профессиональной деятельности использует современное программное обеспечение; – представляет информацию в различных формах с использованием разнообразного программного обеспечения; – способен адаптироваться в новых программных продуктах.	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач. Экспертная оценка документов по учебной и производственной практике.
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	– понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые); – понимает тексты на базовые профессиональные темы; – применяет в профессиональной деятельности инструкции на государственном и иностранном языке; – строит простые высказывания о себе и о своей профессиональной деятельности; – пишет простые связные сообщения на знакомые или интересующие профессиональные темы	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач. Экспертная оценка документов по учебной и производственной практике